

ORIGINAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

FILED
U.S. DISTRICT COURT
NORTHERN DIST. OF TX
FT. WORTH DIVISION

2014 JUL 25 AM 8:48

CLERK OF COURT

UNITED STATES OF AMERICA

v.

CHRISTOPHER ROBERT WEAST

§
§
§
§
§

4:14-CR-0023 - A

DEFENDANT CHRISTOPHER ROBERT WEAST'S
REPLY TO THE GOVERNMENT'S RESPONSE TO MOTION TO FILE
SUPPLEMENTAL DESIGNATION OF EXPERT.

COMES NOW, the Defendant, CHRISTOPHER ROBERT WEAST, by his counsel, Christopher A. Curtis, Assistant Federal Public Defender, and hereby files this reply to the government's response to motion to file supplemental designation of expert in the above styled case, and shows the Court the following:

I.

On July 18, 2014, the defendant filed a motion to supplement its notice of expert by naming Bill McGregor as an expert. The defendant has plainly disclosed to the Court and the government that the defense would like to present the testimony of Mr. McGregor on two primary points: 1) computers are susceptible to remote access and hacking; and (2) it is impossible to look at a visual image and know if it depicts an actual minor. The government has filed a response to this request to designate Mr. McGregor as an expert, has specifically objected to this testimony, and has requested a hearing pursuant to *Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579, 592-93 (1993).

II.

The government objected to the testimony about the possibility of someone remotely

accessing the computer device essentially because experts must tie their testimony to the facts of the case. Government's Response, p. 3, citing the unpublished opinion, *United v. LeBlanc*, 45 Fed. Appx 393 (6th Cir. 2002). As of July 14, 2014, the government's expert provided information concerning a virus scan of the computer in question, requested by the defendant's attorneys. The results of this scan were e-mailed to Mr. McGregor this same date. Mr. McGregor responded in an e-mail at approximately 2:15 pm, that "Looks like most of the hits are java based. I listed a few descriptions below. Looks like it is entirely possible to gain access or load other programs on the computer based on these exploits."

Accordingly, it now appears that testimony concerning someone remotely accessing the computer in this case has been tied to the facts of this case, that is, the virus scan of the computer in question supports the conclusion that remote access is entirely possible on the computer.

Evidence that the computer in question could have been remotely accessed is highly relevant to the element of whether the defendant downloaded the images in question and whether he knowingly possessed the images, as has previously been argued in the defendant's second motion for leave to supplement its designation of experts

III.

The government also objected to the testimony that no-one can possibly tell from viewing an image downloaded off the internet whether that image is an image of an actual person. The government attacks the qualifications of the defendant's expert who lists as a key competency "Forensically image storage on digital devices including computers, mobile devices and video devices." The defendant's expert has a B.S. Degree in Internet System Software Technology, is completing his Masters in Management Information Systems (MSMIS)/ Minor in Digital Forensics,

has an associates degree in Information Systems Technology, and several other qualifications. The defendant has worked for the government on computer systems with Top Secret Clearances.

It appears that essentially the government is arguing that Mr. McGregor is not qualified and has not identified the principles and methods he used to come to the conclusion that no-one can look at a visual depiction that was downloaded on a computer and tell whether that image is an actual minor. Moreover, the government also argues that the technology that exists today might not have existed at the time the images alleged in the indictment were created. However, the very same legislation the government is relying on to prosecute the defendant was based upon findings that are precisely what the defendant seeks to prove to the jury in this case. In fact, findings were made in 1995 when Congress enacted the law that attempted to allow the government to prosecute images that were not of actual minors. The United States Congress, in passing the "A Child Pornography Prevention Act of 1995," made the following findings:

Congress finds:

- ...
- (5) new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from unretouched photographic images of actual children engaging in sexually explicit conduct;
 - (6) computers and computer imaging technology can be used to-
 - (A) alter sexually explicit photographs, films, and videos in such a way as to make it virtually impossible for unsuspecting viewers to identify individuals, or to determine if the offending material was produced using children;
 - (B) produce visual depictions of child sexual activity designed to satisfy the preferences of individual child molesters, pedophiles, and pornography collectors; and
 - (C) alter innocent pictures of children to create visual depictions of those children engaging in sexual conduct;

Child Pornography Prevention Act of 1995, SENATE REPORT NO. 104-358, '2 (August 27, 1996);

see also *id.* at *7, Part I, *8, part III., ' 2, & **15-20, Part IV(b).

Moreover, as long ago as 2001, the Fifth Circuit pointed out that the government's own expert has admitted the very fact that the government now seeks to prevent the defendant from presenting to the jury:

Perhaps most importantly, Congress has advanced a powerful new rationale for the necessity of the "appears to be" language in § 2252A: the need to address the law enforcement problem created by tremendous advances in computer technology . . . , advances that have greatly exacerbated the already difficult prosecutorial burden of proving that an image is of a real child. n33 Without the "appears to be" language in the statute, "there is frequently a built-in reasonable-doubt argument as to the age of the participant, unless the government can identify the actual child involved." n34 During the trial in the instant case, for example, **Special Agent Barkhausen, the government's computer expert, was forced to concede under cross-examination that "there's no way of actually knowing that the individual depicted [in the images] . . . even exists[.]"** The "appears to be" language, then, is necessary to confront the enforcement problems that have been increased by these advancements in computer technology.

United States v. Fox, 248 F.3d 394, 403 (5th Cir. 2001).

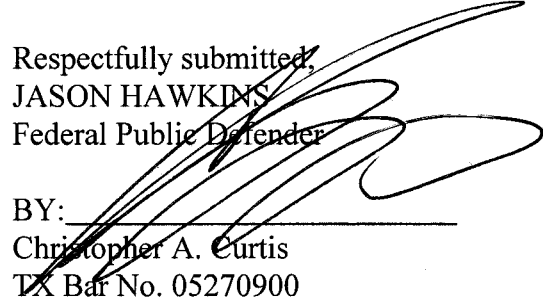
Essentially, the testimony sought from Bill McGregor concerning the images alleged in the indictment – that no-one can testify to the jury with 100 percent certainty that a particular image that was downloaded off the internet is that of an actual minor – is a fact that has been recognized by the United State Congress since at least as early as 1995 and admitted by the government's own computer expert sometime prior to April 13, 2001. However, apparently the recognition of this fact by Congress and one of the government's own computer experts is not reliable enough or scientific enough to satisfy the United States Attorney's Office for the Northern District of Texas.

Interestingly, the defense expects that Mr. McGregor can also testify that one can look at

the "exif data" associated with the images in question and see if there is data showing where the images originated from, although even that data can be manipulated. Often the "exif data" no longer exists on images that have been circulated through the internet. In this particular case, the defense requested the government's expert to check the "exif data" associated with the images in the indictment. None of the images had any "exif data" showing the origination of the image or whether an image had been manipulated except one. That image showed data indicating the image had been handled with "Photoshop 3.0" which, of course, is a program used to manipulate visual depictions.

Wherefore, the defendant prays the Court grant his motion to file a supplemental designation of expert.

Respectfully submitted,
JASON HAWKINS
Federal Public Defender

BY: 
Christopher A. Curtis
TX Bar No. 05270900
Asst. Federal Public Defender
819 Taylor Street, Room 9A10
Fort Worth, TX 76102-6114
817-978-2753
Attorney for Defendant

CERTIFICATE OF SERVICE

I, Angela Saad, hereby certify that on July 25, 2014, a copy of the foregoing reply was e-mailed to Aisha Saleem the morning of July 25, 2014, and was hand delivered to Assistant United States Attorney Aisha Saleem prior to the court hearing at 11:00 a.m. on that same date.



Christopher A. Curtis